

[illegible]

A method and apparatus facilitates the prevention of interception of incoming data, such as keystroke data in the form of a message to an application, by inserting application generated random insertion data into a message stream. The random insertion data is related to actual data that is being generated for a software application so that it is difficult for an attacker to distinguish between actual message data and inserted message data. The system and method then reads incoming data typically in the form of messages, and filters out the messages that it determines were knowingly inserted. The remaining received messages are determined to be actual data from the data source, such as a keyboard, voice input or other suitable data source. In one embodiment, the system effectively hides actual input data such as actual keystrokes in a stream of randomly generated fake keystrokes.